Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 428 BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE EN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN VAN DEFENSIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 november 2016

De afgelopen jaren is het parlement enkele keren geïnformeerd over het gebruik van kwetsbaarheden in hardware en software door de overheid.[1] In het algemeen overleg cyber security op 20 januari jl. heeft de Staatssecretaris van Veiligheid en Justitie naar aanleiding van een vraag van het lid Verhoeven (D66) toegezegd een brief te sturen over het gebruik van onbekende kwetsbaarheden in hardware en software. Naar aanleiding van die toezegging sturen wij u deze brief.

De samenleving digitaliseert en de afhankelijkheid van het internet groeit. Dat biedt grote maatschappelijke en economische voordelen. Tegelijk zijn er zorgen over de mogelijkheid voor bedrijven, burgers en de overheid om op een veilige manier gebruik te kunnen blijven maken van het internet. Veilige computersystemen zijn daarvoor een voorwaarde, en voor het vertrouwen daarin is het van belang het aantal kwetsbaarheden in computersystemen te verminderen. Tegelijk is het voor de veiligheid, zowel fysiek als in de digitale wereld, van belang dat de daders van criminaliteit, terrorisme en spionage worden aangepakt. Daarvoor is het noodzakelijk dat de overheid onderzoek doet in computersystemen, onder meer via het internet. In het streven naar een open, vrij en veilig internet dient aan de diverse belangen recht te worden gedaan. Deze belangen zijn in de meeste gevallen met elkaar in overeenstemming, maar het komt ook voor dat een belangenafweging noodzakelijk is, bijvoorbeeld tussen veiligheid en vrijheden, of tussen verschillende veiligheidsbelangen. Het

[1] Kamerstuk CVIII, N
Kamerstuk CVIII, O
Kamerstuk CVIII, G
Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van het lid Oosenbrug (PvdA), 3 juli 2015, Aanhangsel Handelingen II 2014/15, nr. 2773
Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van de leden Verhoeven en Hachci (beiden D66), 3 juli 2015, Aanhangsel Handelingen II 2014/15, nr. 2772

kst-26643-428
ISSN 0921 - 7371
's-Gravenhage 2016

kabinet hecht dan aan een zorgvuldige afweging die per geval wordt gemaakt. Deze brief behandelt eerst het bestaan van bekende en onbekende kwetsbaarheden en het verhelpen daarvan. Vervolgens wordt de relatie met nationale veiligheid en de opsporing van strafbare feiten behandeld, met bijzondere aandacht voor de bevoegdheid tot binnendringen in geautomatiseerd werk en de daarbij behorende voorwaarden en waarborgen. Tot slot wordt aandacht besteed aan de internationale markt voor kennis over kwetsbaarheden.

Bekende en onbekende kwetsbaarheden

Om een geautomatiseerd werk binnen te dringen is het gebruik van kwetsbaarheden in hard- en software één van de methoden. Indien een kwetsbaarheid bij de desbetreffende fabrikant bekend is, dan kan deze de kwetsbaarheid verhelpen door een update, patch of nieuwe versie van het product uit te brengen. Veel kwetsbaarheden zijn echter niet bekend bij de fabrikant. In dat geval is het voor de fabrikant niet mogelijk de kwetsbaarheid te verhelpen. Onbekende kwetsbaarheden blijven soms jarenlang onopgemerkt. Indien een ander dan de fabrikant een dergelijke kwetsbaarheid vindt, dan wordt dit ook wel een «zero-day vulnerability» genoemd. Een dergelijke kwetsbaarheid kan worden gebruikt om binnen te dringen door software te schrijven die van de kwetsbaarheid gebruik maakt. In dat geval is er sprake van een «zero day exploit».

Het bestaan, de ontdekking en het verhelpen van kwetsbaarheden

Kwetsbaarheden ontstaan bij het produceren van hard- en software, bijvoorbeeld door programmeerfouten of door beperkte aandacht voor veiligheid bij het ontwerp. Hard- en software worden vaak vanwege concurrentieoverwegingen snel op de markt gebracht. Bovendien zijn de omvang en complexiteit van software fors toegenomen. Veel gebruikte applicaties hebben tegenwoordig tientallen miljoenen regels broncode. Kwetsbaarheden zijn daarom talloos en wijdverbreid.

De risico's van specifieke kwetsbaarheden kunnen sterk verschillen. Bij de fabrikant onbekende kwetsbaarheden en het gebruik daarvan krijgen vaak de meeste aandacht in de media, bijvoorbeeld als het software betreft die zeer veel wordt gebruikt. In andere gevallen betreft het zeer specifieke systemen en zijn de kwetsbaarheden vaak lastig te gebruiken. In dergelijke gevallen brengen de kwetsbaarheden vaak minder maatschappelijke risico's met zich mee. Ook reeds bekende kwetsbaarheden kunnen grote risico's met zich mee brengen. Deze zijn vaak bij een grotere groep mensen bekend en kunnen door personen met kwade bedoelingen gemakkelijker worden opgezocht en ingezet.

Veel kwetsbaarheden worden snel nadat ze worden ontdekt gemeld bij de fabrikant. Steeds vaker stimuleren fabrikanten het melden van kwetsbaarheden door het bieden van financiële vergoedingen. Tevens maken veel fabrikanten regelmatig een nieuwe versie of update van hun product, waarmee de op dat moment bekende kwetsbaarheden worden verholpen. Soms duurt het echter lang voordat een fabrikant een update beschikbaar stelt, en soms gebeurt dat in het geheel niet. Het beschikbaar stellen van updates om kwetsbaarheden weg te nemen, is niet verplicht en kan veel tijd en kosten met zich mee brengen. Daarnaast blijken veel eindgebruikers niet of niet direct alle voor hen beschikbare updates te installeren, of ze doen dit niet op de juiste manier. Het gevolg is dat vele systemen niet alleen onbekende kwetsbaarheden bevatten, maar ook kwetsbaarheden die reeds langer bij de fabrikant bekend zijn.

De overheid stimuleert het melden van kwetsbaarheden, onder meer met het beleid voor *responsible disclosure*. Naast voorlichting aan haar partners over door derden gemelde kwetsbaarheden zal het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie (NCSC) in voorkomende gevallen ontdekte kwetsbaarheden zelf melden aan de fabrikant. Ook heeft het kabinet het wetsvoorstel Gegevensverwerking en meldplicht cyber security aan het parlement gestuurd. Dit voorstel bevat een meldplicht voor inbreuken op de veiligheid of een verlies van integriteit van elektronische informatiesystemen bij vitale sectoren.

De nationale veiligheid en de opsporing van strafbare feiten

Criminelen, terroristen en buitenlandse inlichtingendiensten en krijgsmachten maken voor hun activiteiten steeds vaker gebruik van het internet. Die activiteiten zijn zonder onderzoek te doen in het digitale domein steeds lastiger te onderkennen of te bewijzen. Voor een effectieve opsporing, het tegengaan van spionage, verstoring en sabotage, en het waarborgen van de nationale veiligheid is onderzoek in het digitale domein noodzakelijk. Daarvoor zijn in de wet verschillende bevoegdheden opgenomen voor de daarmee belaste diensten. Voorbeelden uit de opsporing zijn het vorderen van gegevens en het onderzoek aan een geautomatiseerd werk tijdens een doorzoeking of na inbeslagname. Dergelijke bevoegdheden zijn voor de inlichtingen- en veiligheidsdiensten vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) en voor de opsporing in het Wetboek van Strafvordering (WvSv). De Wiv 2002 bevat de bevoegdheid tot binnendringen in een geautomatiseerd werk voor de AIVD en de MIVD ten behoeve van de nationale veiligheid. Het wetsvoorstel Computercriminaliteit III bevat wijzigingen in het WvSv voor een bevoegdheid tot binnendringen in geautomatiseerd werk voor vooraf bepaalde opsporingsdoeleinden, voorzien van specifieke voorwaarden en waarborgen.

Technische mogelijkheden

Er zijn verschillende technieken beschikbaar die het binnendringen in een geautomatiseerd werk mogelijk maken. Er zijn vele soorten geautomatiseerde werken en de beveiliging ervan kan vele vormen hebben. Bij de keuze van een methode om het werk binnen te dringen zijn, naast noodzaak, proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning en het risico op gevolgschade van belang. Of het gebruik van een kwetsbaarheid de meest aangewezen methode is, wordt per geval bepaald.

De inzet van wettelijke bevoegdheden voor de nationale veiligheid

Om een zorgvuldige afweging te kunnen maken over de inzet van de genoemde bevoegdheden, is elke bevoegdheid in de desbetreffende wet van specifieke voorwaarden en waarborgen voorzien. Dat geldt ook voor de bevoegdheid tot binnendringen in een geautomatiseerd werk in de Wiv 2002. De bevoegdheid mag alleen worden ingezet in het kader van de nationale veiligheid. De inzet van deze bevoegdheid wordt altijd getoetst aan de eisen van noodzaak, proportionaliteit en subsidiariteit. De inzet moet proportioneel zijn ten opzichte van het doel en het potentiele risico op onbedoelde effecten. Bovendien is de inzet alleen geoorloofd als niet met een minder ingrijpend middel hetzelfde doel kan worden bereikt. De bevoegdheid mag alleen worden ingezet indien vooraf toestemming is verleend door de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de AIVD of de Minister van Defensie voor de MIVD. Daarnaast ziet de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

(CTIVD) toe op de rechtmatigheid van de taakuitvoering van de AIVD en de MIVD. Met het komende voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten beoogt de regering de waarborgen betreffende de inzet van deze bijzondere bevoegdheid verder te versterken.

Op 16 december 2014 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties mede namens de Minister van Defensie het parlement geïnformeerd over de omgang met kwetsbaarheden op internet door de AIVD en de MIVD.[2] De diensten kunnen bij de inzet van bijzondere bevoegdheden kwetsbaarheden in de digitale beveiliging van een target onderkennen en gebruiken. Indien de AIVD of de MIVD in het kader van hun wettelijke taakuitvoering stuiten op een kwetsbaarheid die de belangen van gebruikers van het internet kan schaden, zullen deze diensten belangendragers informeren. Veelal zal het de fabrikant van de hardware of software betreffen en/of een specifieke groep gebruikers die een groot risico loopt.

Er kunnen echter wettelijke bepalingen (de wettelijke plicht tot het beschermen van bronnen, actueel kennisniveau) of operationele redenen zijn die het melden van kwetsbaarheden (tijdelijk) in de weg staan. In dergelijke gevallen wordt het belang van informatieverstrekking afgewogen tegen het belang van geheimhouding en bronbescherming. Voorbeelden van situaties waarin het belang van het melden van een bij de fabrikant onbekende kwetsbaarheid mogelijk niet opweegt tegen andere zwaarwegende belangen zijn de inzet in een gewapend conflict, zwaarwegende belangen voor de nationale veiligheid of als de kennis van een kwetsbaarheid onder voorwaarde van geheimhouding met de Nederlandse overheid is gedeeld. Geconstateerde kwetsbaarheden hoeven niet noodzakelijkerwijs betrekking te hebben op een groot deel van de gebruikers van het internet. Sommige kwetsbaarheden betreffen zeer specifieke systemen. Als het zwaarwegend belang tijdelijk van aard is, dan zal de kwetsbaarheid daarna alsnog worden gemeld.

De inzet van wettelijke bevoegdheden voor de opsporing van strafbare feiten

In het wetsvoorstel Computercriminaliteit III is de inzet in het kader van de opsporing alleen mogelijk voor een beperkt aantal ernstige strafbare feiten en is vooraf toestemming van een rechter-commissaris vereist. De proportionaliteit en subsidiariteit worden zo voorafgaand aan de inzet onafhankelijk getoetst. Politie en justitie hebben, net als in de fysieke wereld, een groot belang bij het voorkómen en beperken van criminaliteit. Het laten voortbestaan van een onbekende kwetsbaarheid kan een risico inhouden op (meer) slachtoffers van criminaliteit. Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen, en waarvan aannemelijk is dat ze nog onbekend zijn, worden in beginsel direct of zo spoedig mogelijk gemeld aan de fabrikant van de desbetreffende hardware of software.

Ook voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen geldt echter dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan. In dergelijke gevallen kan het Openbaar Ministerie, na een zorgvuldige afweging, besluiten de melding van een kwetsbaarheid uit te stellen. Dat kan zich bijvoorbeeld voordoen als de melding zou resulteren in onderkenning van het opsporingsonderzoek door de verdachte of als het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden

---

[2] Kamerstuk CVIII, G

wordt gebruikt. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het Openbaar Ministerie centraal genomen. Daarbij wordt onder meer gelet op de kans dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is. Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software ligt niet in de rede.

De internationale markt voor kennis over kwetsbaarheden

Op internet kan kennis over kwetsbaarheden in hardware en software worden gekocht. Het opdoen van kennis over kwetsbaarheden en de verkoop hiervan is niet verboden. Het beperken van onderzoek naar kwetsbaarheden wordt niet wenselijk geacht. Fabrikanten stimuleren steeds vaker het melden van kwetsbaarheden door het bieden van financiële vergoedingen. Dergelijke kennis kan bijdragen aan de veiligheid van systemen en van het gebruik ervan.

Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de verkoop ervan aan bepaalde partijen onwenselijk. De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen, waardoor het lastig is deze markt aan controle te onderwerpen. Wel is de verkoop van zogenaamde *intrusion software* die gebruik maakt van kwetsbaarheden in bepaalde omstandigheden onderhevig aan exportcontrole. Zoals gemeld in de antwoorden op vragen van de leden Oosenbrug (PvdA) en Verhoeven (D66) van 28 augustus 2015 hecht de regering aan beperking van de uitvoer van ICT-goederen en -software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] De Europese Commissie heeft inmiddels een voorstel gedaan voor herziening van de dual use-verordening waarmee het toezicht op de internationale handel in goederen voor tweeërlei gebruik (dual use) wordt geregeld.

Conclusie

Het kabinet bevordert een vrij, open en veilig internet. Het beperken van kwetsbaarheden in hardware en software is daarvoor van belang. De overheid bevordert het melden van kwetsbaarheden, onder meer met het beleid voor *responsible disclosure*. Het kabinet heeft tegelijk tot taak om binnen de wettelijke kaders de nationale veiligheid te waarborgen en strafbare feiten op te sporen, in de digitale en in de fysieke wereld. Daarvoor is toegang tot digitale informatie noodzakelijk, waarbij in bepaalde gevallen kan worden gekozen voor het binnendringen in een geautomatiseerd werk. Het gebruik van kwetsbaarheden is daarbij één van de technische mogelijkheden om de bevoegdheid tot binnendringen uit te voeren. Deze bevoegdheid is alleen onder strenge, bij wet bepaalde voorwaarden toegestaan en is met specifieke waarborgen omkleed. De

---

[3] Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van de leden Oosenbrug (PvdA) en Verhoeven (D66), 28 augustus 2015, Aanhangsel Handelingen II 2014/15, nr. 3199

noodzaak, proportionaliteit en de subsidiariteit zijn leidend bij de afweging tot inzet. De waarborgen verzekeren een zorgvuldige afweging van de betrokken belangen.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff

De Minister van Binnenlandse Zaken en Koninkrijksrelaties
R.H.A. Plasterk

De Minister van Defensie
J.A. Hennis-Plasschaert